

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)
13-04-2015

2. REPORT TYPE
Master's Thesis

3. DATES COVERED (From - To)
21-07-2014 to 12-06-2015

4. TITLE AND SUBTITLE

Cyber and the American Way of War

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR

Lieutenant Colonel Lisa Nemeth, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College
Joint Advanced Warfighting
School 7800 Hampton Blvd
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The American way of war has been discussed in literature since the concept emerged in 1973. Since that time, effects of integrating cyber activities into the concept of warfare have not been addressed surrounding the conceptualizations of the American way of war. This paper examines the current literature to create a characterization of the American way of war and then proposes how cyber will change the American way of war.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT
Unclassified

b. ABSTRACT
Unclassified

c. THIS PAGE
Unclassified

17. LIMITATION
OF ABSTRACT
Unclassified
Unlimited

18. NUMBER
OF
PAGES
40

19a. NAME OF RESPONSIBLE PERSON

19b. TELEPHONE NUMBER
(include area code)

757-443-6301

Intentionally left blank

NATIONAL DEFENSE UNIVERSITY
JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL



CYBER AND THE AMERICAN WAY OF WAR

by

Lisa Nemeth

Lt Col, U.S.AF

This page intentionally left blank.

CYBER AND THE AMERICAN WAY OF WAR

by

Lisa Nemeth

Lt Col, U.S.A.F.

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes. (or appropriate statement per the Academic Integrity Policy)

Signature: 


March 24, 2015

Thesis Advisor:

Signature: 
Dr. Sterling M. Paye, Associate Professor

Approved by:

Signature: 
CAPT S. M. Gulliani, USN
Committee Member

Signature: 
Dr. Robert Antis
Acting Director, Joint Advanced Warfighting School

This page intentionally left blank.

ABSTRACT

The American way of war has been discussed in literature since the concept emerged in 1973. Since that time, effects of integrating cyber activities into the concept of warfare have not been addressed in discussions surrounding the conceptualizations of the American way of war. This paper examines the current literature to create a characterization of the American way of war and then proposes how cyber will change the American way of war.

ACKNOWLEDGEMENTS

Thank-you to COL (ret) Jerome Hawkins for his review of my paper and identification of areas that needed clarification.

Table of Contents

Introduction.....	1
The American Way of War.....	3
The American Military Way of War.....	3
Overwhelming Force/Decisive Victory	4
Advanced Technology	6
Independent Action	7
War is Against Military Forces.....	8
Summary	9
The American Political Way of War.....	9
The Use of Force.....	10
Risk and Aversion to Casualties and Collateral Damage	13
Whole of Government Approach to War?	15
Summary	17
Cyber and the American Way of War.....	17
What Will Not Change / How Cyber Fits into the American Way of War	19
How Cyber Warfare Should Alter the American Way of War.....	19
Whole-of-government Approach to War	20
A New Civil-Military Relationship	24
Use of Force Concepts	26
Military Forces, Civilians, and Collateral Damage	28
Conclusion	34
Bibliography	36
Vita	40

Introduction

The idea of an American way of war came into existence in 1973 with the publication of Russell Weigley's, *The American Way of War*. According to Weigley, the American way of war was more a way of battle and followed a strategy of annihilation.¹ Weigley's work and conclusions were initially accepted as definitive, but after the First Gulf War historians began debating Weigley's conclusions. In a recent work, *Reconsidering the American Way of War*, Tony Echevarria breaks the literature of the topic into three phases.² The first phase is Weigley's study and surrounding discussion. Phase two began in the mid-1990s and lasted until after the invasion of Iraq in 2003. In this phase, historians worked to integrate new technologies and resultant changes in the methods of war. Finally, Echevarria's third phase begins with the pre-surge difficulties the United States experienced in Iraq in 2003 to 2005 and examined the American way of war for a cause.

What has not yet appeared is a phase four—an attempt to describe the American way of war that includes cyber actions in warfare. Today there are different schools of thought as to what impact cyber will have on war and warfare. Some theorists do not think that cyber warfare will cause substantive changes to the American way of war as it is only another technology. Others believe it is part of the ongoing information revolution already captured in the way of war debate. Still others do not address cyber at all. Recent international headlines on cyber activities and its potential as a medium for

¹ Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (1973; repr., Bloomington: Indiana University, 1977).

² Subsequent phases outlined by Antulio J. Echevarria II, *Reconsidering the American Way of War: U.S. Military Practice from the Revolution to Afghanistan* (Washington, D.C.: Georgetown University Press, 2014), 10-11.

coercion demonstrate how integral cyber is to society today. Cyber actions can no longer be ignored—no matter how uncertain its future—when examining the conduct of national security and warfare.

This paper will begin that discourse. It will demonstrate that the addition of actions in cyberspace to warfare will alter the American way of war.

This paper consists of two major sections. The first will review existing literature and trends to determine characteristics that define the American way of war. Part two will take this characterization of the American way of war and outline the affect cyber activities in warfare will have on the characteristics and thereby on the American way of war.

The American Way of War

There are many definitions of the American way of war. It is difficult to make direct comparisons among them as the definitions focus on different conceptual levels of war. The definitions range from pure military characterizations of the American way of war to global-strategic definitions that attempt to explain how the American government views and uses war. What is clear from all of these efforts is, as Benjamin Buley writes: “There is no single American way of war or consensus over the proper relationship between war and national policy.”³ To further compound the comparative difficulties, some definitions were written not to simply describe the American way of war, but for the purpose of explaining a specific war’s outcome. Others, as Brian Linn points out, were written only considering war years, ignoring peacetime activities and therefore do not provide a comprehensive definition.⁴ In order to create a useful understanding out of this abundance of ways of war, this paper will take a new approach. The American way of war will be examined first from a military perspective and then from a national-strategic or government-level perspective. In each category, commonly agreed-upon characteristics of the way of war will be outlined to weave a new characterization of the American Way of War.

The American Military Way of War

Historian Dr. Lawrence Sondhaus noted that, “the American tendency to focus on the practice of war rather than the broader conceptualization of it thus colors the literature

³ Benjamin Buley, *The New American Way of War: Military Culture and the Political Utility of Force* (New York: Routledge, 2008), 6.

⁴ Brian McAllister Linn, *The Echo of Battle: The Army's Way of War*. (Cambridge, Massachusetts: Harvard University Press, 2007), 233-4.

on the American way of war.”⁵ Dr. Sondhaus’ description is apt, for many characterizations of the American way of war are centered on the military aspects of war, or rather, on how war is fought. Therefore, this paper will explore the military facet of the American way of war first. The reader must be cautioned not to interpret what follows in this section as the American way of war, for this section will address a way of war as defined by the American military without inputs from other American entities. This fragmentation of the American way of war may be more of an ideal desire of the military, as it tends toward how the military desires to fight its wars in absence of governmental control over strategies, acquisitions or actions. Nonetheless, the elements presented create a characterization of the way the American military fights wars and will form a foundation to later explore the integration of cyber warfare.

Within this military-focused exploration of the American way of war, there are four dominant characterizations that emerge: the desire to use overwhelming force to achieve a decisive victory, the use of advanced technology, the desire for independence from politics, and a focus on opposing military forces.

Overwhelming Force/Decisive Victory

In his study of *Ethics, Technology and the American Way of War*, Ruben Brigety describes two dominant themes of American practice, the first of which is “a tendency to seek decisive victory through the overwhelming use of force.”⁶ As he notes, this concept reaches back to Weigley and his original characterization of the American way of war as

⁵ Lawrence Sondhaus, *Strategic Culture and Ways of War* (New York: Routledge, 2006), 62.

⁶ Reuben E. Brigety, *Ethics, Technology and the American Way of War: Cruise Missiles and US Security Policy*, (New York: Routledge, 2007), 37.

annihilation.⁷ These concepts form a common theme among historians describing the American dislike for long-drawn out wars of attrition while preferring large-scale, aggressive, offensive actions in war. These ideas are consistent throughout many definitions of the American way of war. Recently however, theorists have started to shift away from this conclusion. Eliot Cohen, for example, puts the desire for a decisive battle as the old way of war with a shift occurring around the Kosovo War.⁸ Likewise, Benjamin Buley also categorizes these characteristics as the old way of war for America.⁹

If this is the old way as many theorists are starting to assert, then what is the current American way of war? In 2004, Echevarria wrote that the American way of war still retained the concept of “rapid decisive operations.”¹⁰ However, in 2014 he revisited the topic and modified his view. His new concept is that while the American way of war still “places decisive operations at the core of its conception of war,” Echevarria concludes that the United States, “rarely employed overwhelming or decisive military force,” throughout its history, applying instead only “sufficient means” or credible force.

¹¹ In this conclusion, Echevarria touches on a dichotomy also noted by Cohen. This desire for overwhelming force and a decisive battle is a “statement of ideal conditions...what war ought to be more than what it has actually been.”¹² While America prefers to overwhelm their opponents and defeat them in a decisive battle, that is not how America actually fights the majority of the time.

⁷ Ibid., 37.

⁸ Eliot Cohen, “Kosovo and the New American Way of War,” in *War over Kosovo: Politics & Strategy in a Global Age*, ed. Andrew J. Bacevich and Eliot Cohen (New York: Columbia University Press, 2001), 42 & 45.

⁹ Buley, 1.

¹⁰ Antulio J. Echevarria II, *Toward an American Way of War*, (Carlisle: Strategic Studies Institute, 2004).

¹¹ Echevarria, *Reconsidering the American Way of War*, 4 & 167-169.

¹² Cohen, 45.

If overwhelming force and decisive battle is the ideal Americans still strive to achieve, or as some advocate, the previous way of war, what is the reality? Buley summarizes it best: “achieving ‘systemic paralysis’ of the enemy’s armed forces and infrastructure rather than their annihilation.”¹³ To most of the American public, this is also known by another phrase: shock and awe. The desire to quickly overwhelm the enemy still exists—without necessarily using overwhelming force in a decisive battle.

Advanced Technology

The ability of the American way of war to ‘shock and awe’ its opponents is enabled by what Max Boot believes characterizes the American way of war: speed, maneuver, flexibility, and the use of surprise to achieve quick victory, all of which are created by a reliance on technological advances.¹⁴ This is the second characteristic of the American way of war—reliance on technology. Oft cited examples of America’s dependence on technology include the use of smart munitions, networks and information systems at the center of operations. Colin Gray creates a broader description of the use of technology in his characteristics of the American way of war. He states that the U.S. military is “culturally attuned to favoring technological solutions over other approaches.”¹⁵ The importance of technology to the American way of war leads Brigety to list it as his second dominant theme after the use of overwhelming force in a decisive battle when he describes the American desire for the: “quest for technological superiority *vis-à-vis* an enemy, and the propensity to apply technological solutions to strategic

¹³ Buley, 2.

¹⁴ Max Boot, “The New American Way of War.” *Foreign Affairs* 82, no. 4 (July - August 2003): 42.

¹⁵ Colin S. Gray, “Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?” In *Irregular Warfare: Strategy and Considerations*, ed Arnold Milton and Walt Berkovski (New York: Nova Science Publishers, 2012), 112.

problems.”¹⁶ The American way of war places technology at its center, using it to solve battlefield and strategic problems.

Independent Action

Another common description of the American military’s way of war is their preference and belief that they should be told what to achieve by the politicians and then left on their own to accomplish the tasks. As Buley states: “commanders have accepted the sovereignty of political objectives in principle, yet have still sought to preserve a realm of purely military decision-making free from the intrusion of political considerations.”¹⁷ This conflict arises because, in practice the military views strategy as a “doctrinal process,” while policy, which informs strategy is often “the product of negotiation and compromise”—a non-linear and somewhat irrational process directly in conflict with military process and thought.¹⁸ This drives a separation in processes where as Cohen states, the politicians set “objectives that victory in battle would secure” and “once those objectives were defined, Americans preferred to keep politics as far apart from war as possible.”¹⁹ Again, as with the other characterizations, this is more a desire rather than reality as civilian politicians commonly exert control over target lists, troop numbers, and make significant input into military strategy and operations. Additionally, as America demonstrated in recent wars and Cohen argued in 2004: “objectives must be

¹⁶ Brigety, 38.

¹⁷ Buley, 11.

¹⁸ Frank Hoffman, “Politics and the American Way of War (and Strategy)” War on the Rocks. Entry posted November 2013, <http://warontherocks.com/2013/10/politics-and-the-american-way-of-war-and-strategy/> (accessed September 3, 2014)

¹⁹ Cohen, 49.

adjusted in accordance with political exigency, changing moods and preoccupations...and consequences of success and failure on the battlefield.”²⁰

Aside from separation from the politicians in wartime, the military desires its independence between wars as it shapes itself for future wars. As Linn elaborates there is a “deeply cherished belief among America’s military personnel that, if left alone, the armed services would reform themselves.”²¹ Although Linn was referring to the post-Civil War period, scholars echo the same sentiment for every major conflict or military drawdown. It is even prevalent today as the armed forces prepare for their vision of future conflicts and incorporate lessons learned from Iraq and Afghanistan, while working within imposed budget restraints.²² The military, once given its task, expects to determine its own actions free from political interference, whether structural or in a conflict.

War is Against Military Forces

The final characteristic common to the various definitions of the American military way of war is the military’s focus on the opposing military forces. This is a traditional, western view of war, now formally upheld by the Geneva Conventions. Even without the legalities, in its way of war the United States prefers to limit violence to the opposing military.

As industrialization expanded and civilians became essential to the war effort and the army’s ability to function and fight, America’s preference to only target military forces remained. Intentions aside, as Wayne Lee demonstrates, as a war progressed and

²⁰ Ibid., 49.

²¹ Linn, *The Echo of Battle*, 41.

²² E.g., the current battle between the U.S. Air Force and Congress over retiring the A-10.

the desire for unconditional surrender grew, historically America would increase violence, often targeting the enemy's infrastructure.²³ Collateral damage was not desired, but was accepted. However, since WWII and the creation of the current Geneva Conventions and Protocols, "citizens are increasingly described as fundamentally innocent."²⁴ This created a strategic dilemma between military necessity and protection of civilians for which the American military turned to technology and precision to solve as the military strives to only attack military targets.²⁵ Today the U.S. military continues to go to extraordinary lengths to avoid targeting civilians while maintaining its actions in war only against opposing military forces and military infrastructure. This is not just a military attribute of the way of war, as this characterization will be further expanded in the next section.

Summary

Using commonly agreed upon characteristics in the way historians define the American way of war, a way of war emerges as one that overwhelms its opponents in hopes of creating a quick and decisive defeat through the use of advanced technology. The military prefers that the political decision makers define objectives but then ultimately allow the military to operate on its own to achieve the specified objectives, which it prefers to accomplish by focusing on the enemy's military forces.

The American Political Way of War

The other approach to the American way of war considers it at the national governmental level. Here, the focus is on how war is used and the political

²³ Wayne E. Lee, *Barbarians & Brothers: Anglo-American Warfare, 1500-1865*, (New York: Oxford University Press, 2011), 243-244.

²⁴ *Ibid.*, 245.

²⁵ *Ibid.*

considerations involved in the use of force. Compared with the military characterizations, the political governmental characterizations do not have as clear of a consensus on the traits of the American way of war. Nonetheless, it is possible to identify commonalities from the literature. These are how America uses force, the nation's thoughts on risk, casualties and collateral damage, and how the military use of power is integrated into America's overall policy.

The Use of Force

At its core, the idea of a national way of war is how force is used in relation to diplomacy and politics. Much has been written on this aspect of the American way of war, often with reference to American strategic culture. Despite the amount of literature, there is not a single agreed-upon description of how America views the use of force. Authors instead present many discordant ideas. However, within the distinctions, common themes emerge.

A common descriptor of America's way of war is that America does not have an understanding of the relationship between war and peace. This relates to the military side of the way of war, as Buley describes, America prefers "to distinguish sharply between the states of peace and war, and once committed to the latter, to mobilize the republic's abundant resources behind an offensive of the highest possible intensity."²⁶ Echevarria notes the same concept when he states that Americans "consider war an alternative to bargaining, rather than part of an ongoing bargaining process."²⁷ In other words, politics

²⁶ Buley, 2.

²⁷ Echevarria, *Toward an American Way of War*. 1. Echevarria continues: "In other words, the American concept of war rarely extended beyond the winning of battles and campaigns to the gritty work of turning military victory into strategic success."

and diplomacy end (or fail) and war begins. Peace and war are viewed as binary alternatives and do not exist together.

Unfortunately, when war ends and peace begins is also not cogent for America, for the American way of war is also described as forgetting that an important part of war, and the use of force, is determining the peace that follows. The common theme in the literature is that for America, war is conducted with the aim of achieving military victory. America gives scant thought to the fact that how war is fought and what happens in war will affect the strategic landscape post-conflict, specifically the achievement of political victory. America believes that victory in war will itself bring the desired peace. But the reality is more complex; what happens during war determines the course and context of the peace that follows. While this theme is prevalent throughout the literature on the American way of war, Colin Gray is one of the more vocal authors on this issue. Gray puts part of the cause for America's failure in the "nation's traditional theory of civil-military relations which discourages probing dialogue between policymaker and soldier."²⁸ Echevarria concurs with Gray's assessment and describes the American system as "encouraging power and diplomacy to occupy separate spheres."²⁹ This division is strong in American tradition. The military desires to conduct war free from political interference. Nonetheless, the military is not the sole source of this civilian-military divide as many historians are quick to show that the civilians are equally culpable. While the military wants to operate independently and as it deems best to achieve the nation's objectives in war, civilians at times tend to "distance themselves from the realities and limitations of force, or avoid asking hard questions about how

²⁸ Gray, "Irregular Enemies and the Essence of Strategy," 108.

²⁹ Echevarria, *Toward an American Way of War*, 13.

proposed “ways” relate to the desired ends.”³⁰ This split creates a situation where the conduct of the war is placed predominately in the domain of the military with civilians relying on the military to achieve the political goals. The focus becomes winning the military conflict and not necessarily setting conditions for the peace that follows and thus characterizes the American way of war.

Many scholars note that the military-political divide and thereby the American dichotomy between the states of war and peace has been diminishing since the end of the Cold War. An especially popular topic post Iraq, this change served as the focus of many of the more recent studies of the American way of war.³¹ Even with an overall consensus of progress, Echevarria opines that despite the lessons of Iraq and Afghanistan, the American way of war has not shifted from a focus of “defeating the enemy in battle.”³² Buley also states that the U.S. has recently “acknowledge[d] that the conduct of strategy should be governed by the political objective, but they [policymakers in America] still sought both to restrict that objective to one that could be neatly achieved through the massive application of military power, and to maintain a realm of purely military decision-making that could remain unsullied by political considerations.”³³

Despite these condemnations of any changes, there is some progress in recent thought on how war affects the peace. While primarily designed to defeat the enemy, the surge and how it was conducted in Iraq also focused on strategic level outcomes. The concept was created together by the military and politicians. Military professional

³⁰ Hoffman.

³¹ This is an outcome of Echevarria’s third phase of the study of the way of war. See Buley. Echevarria has also revisited his previous view on the topic by stating in his most recent book that the American uses of force have always been driven by political considerations, yet notes that the way of war still retains its battlefield victory focus.

³² Echevarria, *Toward an American Way of War*, 16. Also Echevarria, *Reconsidering the American Way of War*, 174.

³³ Buley, 14.

education spends many hours of instruction over the linkage between strategy, politics and military operations. Yet, despite these changes, no author states that the overall American way of war has changed. Buley describes the ongoing debate in America as contextual to a type of war rather than to all wars in general. He questions, “whether the form of warfare...in which military and political considerations are inextricably intertwined will increasingly be the exception or the norm.”³⁴ However, Gray and others would advocate that this pervasiveness of politics in war (and its effect on the following peace) is not limited to a type of war but is present in all war.

Irrespective of this debate, what is unquestionable is that there is a realization within America that the previous divide between the states of war and peace is not appropriate.³⁵ However, there still remains uncertainty and friction in how America defines the relationship or how it creates a bridge between war and politics as it attempts to reconcile its way of war with its tradition of a military-civilian divide. Today, the American way of war may view war as a political instrument, but America’s conduct of war does not yet carry this view through to its actions. Therefore the American way of war still “wage[s] war as a largely autonomous activity, leaving worry about peace and its politics to some later day.”³⁶

Risk and Aversion to Casualties and Collateral Damage

America has not only experienced changes in the political context of the use of force but also in the application of force. Regardless of America’s experience and history in the types of wars it has fought, America “has displayed a strong and long-standing

³⁴ Ibid., 139.

³⁵ Ibid., 140-146. Also Hoffman.

³⁶ Gray, 108.

predilection for waging war for unlimited political objectives.”³⁷ However, the advent of the nuclear age and the subsequent Cold War forced America to focus more on limited wars. Limited wars provided “concrete, well defined objectives that do not demand the utmost military effort”, and also had the added benefit of permitting “economic, social, and political patterns of existence to continue without serious disruption.”³⁸ Limited wars were desirable for the United States as it advanced its national interests while maintaining political support at home. Therefore “policymakers opted for a strategy of limited war in which the use of force was measured in scope and intensity in order to achieve a very specific objective at an acceptable cost.”³⁹

What America found as it fought limited wars was that to maintain the necessary national and international support, military actions were constrained to limit American military casualties and collateral damage.⁴⁰ While Colin Gray questions whether this is really a requirement, he does concur that the United States has inculcated this aversion as part of its way of war.⁴¹ As a consequence, America has sought to exert control over war itself, to try to make it predictable in order to reduce risk while preventing casualties and collateral damage. A concept noted by many authors, Linn sums it up best in that America shows: “the propensity to view war as an engineering project in which the skilled application of the correct principles could achieve a predictable outcome.”⁴² Again, as mentioned earlier, America embraced technology to solve this dilemma.⁴³

³⁷ Thomas G. Mahnken, *Technology and the American Way of War* (New York: Columbia University Press, 2008), 4.

³⁸ Robert Osgood as quoted in Brigety, 48.

³⁹ Brigety, 132.

⁴⁰ Ibid., 129, however this is common in much literature on the American way of war.

⁴¹ Gray, “Irregular Enemies and the Essence of Strategy,” 122.

⁴² Linn, *The Echo of Battle*, 199.

⁴³ Buley, 14; Linn, *The Echo of Battle*, 199; Gray, “Irregular Enemies and the Essence of Strategy,” 112-113, 121-122.

Precision guided munitions, small diameter bombs, Tomahawk missiles, and drones all seek to limit casualties and collateral damage and have become characteristic of the American way of war. This optimistic view about the management of war is the subject of many critiques of the American way of war, primarily focused on the flaw in the American belief of the ability to keep war in a strict military realm while ignoring the political aspects.⁴⁴ Others, such as Michael Ignatoff do not address the military-political divide, instead arguing that this avoidance of risk and casualties allows the U.S. President easier use of military force, thereby bypassing other aspects of national power.⁴⁵ Still others advocate that technology allows the military to solve the casualty and collateral damage problems, taking a humanitarian approach to war which it can then use as a weapon against its enemies as well as a way to garner international support.

The political context of limited wars as well as increasing international and national sensitivity to collateral damage in wars has given rise to an American desire to control the effects of war. Technology is viewed as the means to limit collateral damage. As demonstrations of precision increasingly became the norm, the consequence has been an increased sensitivity to military casualties and collateral damage. Over time, this sensitivity has been inculcated into the American way of war, which is now characterized as unaccepting of casualties and adverse to collateral damage.

Whole of Government Approach to War?

The civilian-military separation within the American system does not only apply to the divide between the military and American political leaders. Historically, the

⁴⁴ For example, see Buley, 14.

⁴⁵ Michael Ignatieff, "The New American Way of War" *The New York Review of Books*. July 20, 2000. <http://www.nybooks.com/articles/archives/2000/jul/20/the-new-american-way-of-war/?insrc=toc> (accessed October 23, 2014), 2.

military is also routinely separate from other elements of national power, government agencies, and their execution organizations. This was an oft-cited reason for the failure of the United States in Iraq and Afghanistan—the United States failed to take a whole-of-government approach and coordinate the actions of each governmental arm. The military has relationships with the various intelligence agencies, relationships that have increasingly improved since 9-11. Likewise, the military also has ties with some agencies of the Department of Homeland Security. However, interaction with the diplomatic and economic arms of the U.S. government has traditionally been deficient. This has significant effect on the American way of war. To reiterate, the American way of war is to use the military to achieve the government's objectives. All governmental agencies support that effort, but they are not responsible for the execution of the conflict itself.⁴⁶ As the American conceptualization of war has evolved from being seen as primarily a force-on-force endeavor, the categorization of war strictly as a military issue is increasingly out of context. This became apparent to the U.S. Government in recent U.S. actions and has generated much debate. Recent recognition of the necessity of a whole-of-government approach does not yet rewrite the characterization of the American way of war, however this aspect appears to have the firmest realization that it needs to change. It is yet to be seen if the American system can make the adjustments to change its way of war.

⁴⁶ Specifically referring to limited wars. There may be fall-out or ancillary duties that affect the agencies, such as intelligence or increased homeland security, but the agencies are not responsible for success or failure in the war. Granted, the State Department does play a significant role in building and maintaining international coalitions and global diplomacy.

Summary

The American governmental way of war complements the military view. As a whole, America prefers to keep separation between the political direction of war and the military's execution of it. This contributes to the American view of peace and war being binary, in which both are separate conditions. Finally, America is casualty adverse, both with its military and civilians as well as shy of collateral damage. This has led the nation to use technology to attempt to manage war and thereby limit the damage of war. It has also created world expectations of the America's ability to do so at all times. Finally, historically, America limits war to the realm of the military rather than taking a whole-of-government approach to war's conduct.

Each of these characteristics of the American way of war has been challenged by recent American wars. The shortcomings were apparent during recent conflicts and individuals within the American military and government realize that these characterizations of the American way of war must change in order to achieve lasting victories. Nonetheless, the realization that changes are needed is not enough to actually force changes. Now that the crisis of the most recent wars seems passed, America has demonstrated tendencies to revert to its traditional characteristics of the American way of war.

Cyber and the American Way of War

No longer a nascent technology, recent cyber events have demonstrated the ability to halt daily functions in a society, execute a very precise attack with a specific effect,

and cause hundreds of millions of dollars in damages to corporations and nations.⁴⁷ Each of these events has exhibited different attributes associated with cyber attacks: pre-emptive, surgical/aesthetic, deterrent, escalatory, unacknowledged/non-attributed, coercive, and/or pervasive. Each attack was also against non-military systems and in some cases, privately owned infrastructure, systems or entities. This wide range of characteristics for cyber actions does not create a clear future for the integration of cyber into warfare. In total war where unconditional surrender is the goal, the use of cyber could be rampant with its effects pervasive throughout the societies in conflict. However, in limited war or peacetime conflict, cyber's role and expected level of use remains the subject of much debate.

For America, the future path of cyber in warfare and the American way of war are intertwined. The American way of war will shape cyber's role in warfare, and in turn, cyber actions will affect the American way of war. This is because the current American way of war controls how America views the possibilities of cyber in warfare and determines what tools, techniques, procedures and technologies are developed to support its use. The lessons learned as that process unfolds will in turn alter the American way of war. Cyber's omnipresent nature in society distinguishes it from other domains in warfare and creates far-reaching implications from the addition of cyber actions into warfare. Despite the uncertainty surrounding its ultimate role, the integration of cyber into warfare will place pressure on the American way of war to change. This section discusses some of the future implications of cyber in warfare to the American way of war.

⁴⁷ In order: Estonia and Georgia, Stuxnet, and Sony Pictures. Some estimates quote loss and recovery costs for Sony as over half a billion dollars.

What Will Not Change / How Cyber Fits into the American Way of War

Two aspects of the American way of war are congruent with cyber warfare. First, the American military's reliance on technology to fight wars and solve its strategic problems aligns perfectly with cyber as cyber is technology and presents new methods to solve both old and new problems in war. Likewise, cyber is perceived as a fit with the American desire for overwhelming force, decisive victory, and the newer perspective of achieving system paralysis. Here, cyber is viewed as enabling or directly contributing to the creation of these attributes of the American way of war. One could even argue that attaining systems paralysis will not be possible without cyber in warfare, as information technology has become integral to warfare in almost every form.⁴⁸ Because cyber presents a new technology that has potential to solve problems in war and also has potential as a method to create strategic paralysis and thereby decisive victory against an opponent, the addition of cyber will not likely affect these characteristics of the American way of war. The American way of war will still continue look to technology to solve its dilemmas and to achieve decisive victory and will use cyber actions to do so.

How Cyber Warfare Should Alter the American Way of War

While cyber actions in warfare may be congruent with some aspects of the American way of war, it has the potential to create profound changes in other characteristics. Specifically, the addition of cyber in warfare will place pressure on the ability of the military to be given objectives and act independently to achieve them. This will further shift the American way of war into an integrated whole-of-government approach to war. The addition of cyber actions in warfare will also increase civilian

⁴⁸ Even most non-technical adversaries rely on cyber (and information technology) for financing, recruitment, communication and influencing public opinion.

involvement in military operations. Furthermore it will eliminate the binary distinction between the states of war and peace existing in the American way of war and thereby end the apolitical tendency of the American way of war. Finally, the inclusion of cyber actions will require the American way of war to adjust to an increased uncertainty regarding collateral damage and the civilian casualties associated with warfare. This section will illustrate the effect on each of these characteristics of the American way of war.

Whole-of-government Approach to War

Just as Iraq and Afghanistan brought other U.S. Government agencies into the American conduct of war, the addition of cyber into warfare will take the relationship further. Today multiple governmental agencies are necessary to achieve objectives in the quest for victory. This whole-of-government approach is common policy in most contemporary military actions and has been codified through various Presidential directives in recent years. The current Department of Defense Cyber Strategy for Operating in Cyberspace is in line with this concept: “In order to enable a whole-of-government approach, DoD will continue to work closely with its interagency partners on new and innovative ways to increase national cyber security.”⁴⁹

While acknowledging the necessity of a whole-of-government approach, current DoD strategy only refers to interagency cooperation in terms of sharing ideas, sharing of capabilities, and supporting collective efforts for cybersecurity.⁵⁰ The inclusion of cyber actions in warfare into operational concepts will require a change in these relationships. The addition of cyber into warfare will create the need for a multi-agency approach to

⁴⁹ U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, (2011), 8.

⁵⁰ *Ibid.*, 8.

war planning and execution, going beyond aligned objectives and coordinated agency roles. Instead, cyber will require that agencies are party to decisions, in both planning and execution. In short, whole-of-government becomes more than just coordination of efforts, idea sharing and acknowledgement that each agency's effort is required. Whole-of-government becomes an integrated team. For the American way of war, this means that not only are policy-makers involved with the establishment and execution of military objectives, but that many other government agencies are involved as well.

The cause for this shift in response to cyber is two-fold. First, cyber is not solely the domain of the military. It is pervasive across modern society. The internet, networks, and thereby, cyber, relies on non-military components. Robert Latham uses the term "dual-coded" to refer to information technology infrastructures, which have become a core infrastructure for all of society, not just for the government and military.⁵¹ It is not possible for the military to use only military infrastructure. It may not even be possible to use only American infrastructure as the internet is decentralized with components across the globe. Any attempts to affect the network or its components can therefore have direct or indirect effects on other agencies, private organizations or individuals.

Second, with cyber there are only fleeting concepts of national borders or territory. As many have noted, the use of cyber has the effect of ending the distinction between internal and external security for a state. Chris Demchak provides a good discussion on this topic in her essay "*Cybered Conflict, Cyber Power, and Security*

⁵¹ Robert Latham, "Introduction" In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. ed. Robert Latham (New York: The New Press, 2003), 13-16.

Resilience as Strategy".⁵² Historically in the west, she argues that the military was responsible for external security—keeping dangers out of the nation—while police and other agencies were responsible for security within the borders. In response to this internal/external division, nations developed "concepts, strategies, and institutions" to create internal and external security.⁵³ Cyber, with its lack of geography and ubiquitous nature, allows threats to "reach directly into societies" bypassing military forces, thereby challenging this internal/external division.⁵⁴ America is no different. The integration of cyber challenges the existing division of security responsibilities and roles as well as how the nation thinks about security.⁵⁵ Consequently, America's recent whole-of-government efforts may not go far enough to allow its military and agencies to provide security in a world where internal and external security are blurred.

The change to an integrated governmental approach to cyber is not only for conceptual reasons. As a result of cyber warfare, adversaries can, with low barriers to entry, gain necessary tools to conduct offensive operations anywhere inside American borders. Practically speaking, actions taken by America's military in a conflict—cyber or physical—may now lead to direct and immediate effects on the American homeland or to other agencies' operations through cyber-based counter-attacks. Retribution could drive focused cyber attacks on agencies or private entities that have no warning due to the nature of current division of operations within the government. With cyber as a form of warfare, American military actions are no longer isolated to the region where there is

⁵² Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012).

⁵³ Ibid., 131.

⁵⁴ Ibid., 129 & 131.

⁵⁵ Demchak, 127-131. See also Latham, "Introduction", 11.

physical fighting but can have reciprocal effects anywhere in the homeland or around the world.

Homeland defense and the consequences of a counter-attack are not the only reason cyber will drive a greater whole-of-government approach. Cyber operations conducted by the military can have a direct effect on other governmental agencies' activities. Various agencies may have conflicting ideas how best to exploit vulnerabilities in adversary systems. For example, if multiple government agencies were planning on using a known deficiency in an enemy network to gain access to systems, the use of that entry point by one agency can permanently close it to others. It could even affect access to other systems in that nation as security levels and awareness change in response. Cyber is unique in that once an access point is used and the enemy traces how their systems were affected, they can patch that weakness thereby preventing other attacks or entries at that point. Essentially, if an avenue is used and the enemy becomes aware, the future landscape for cyber operations is altered. Furthermore, agencies without cyber capabilities might have conflicting ideas about what could be gained through exploitation.⁵⁶ A whole-of-government approach is needed to centrally identify cyber weaknesses, overlapping interests, and coordinate their use.

There are further implications for homeland defense in cyberspace. Once a weakness is identified via exploitation, that vulnerability becomes available to the black hat community for alteration and exploitation. If the code were to spread beyond the targeted systems, there could be unintended spillover or blowback into American systems, both government and private. Such spillover or blowback can cause direct

⁵⁶ Herbert Lin. "Operational Considerations in Cyber Attack and Cyber Exploration" In *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 50.

effects if the code affects American systems, or indirect effects if, for example, the malicious code had resultant effects on the economy or infrastructure.⁵⁷ Therefore, knowledge of vulnerabilities needs to be shared to defend against or to rapidly respond to attacks.⁵⁸

The combined effects of integrating cyber into warfare create a situation where the military can no longer independently plan and execute war. As internal and external security merge into one, so must the actions of the agencies previously responsible for each component of security. To create the best homeland defense and to take advantage of cyber opportunities for offensive action, the military must not only coordinate but must integrate its actions with other government agencies. With cyber warfare, the American way of war can no longer be to assign objectives to the military and have the military achieve them with only basic coordination among other agencies. Instead, military action must be integrated step-by-step throughout the government. Cyber warfare forces the American way of war to involve the entire government, and no longer permits independent action of the military.

A New Civil-Military Relationship

The integration of cyber warfare will also affect the civilian-military relationship in America. The military will have to accept further civilian involvement in operations. Civilians will also need to engage more with military operations.

This change will create friction. The military already feels they have less independence to conduct war than they should. Cyber warfare will further restrict their independent operating space, as political decision makers find that military operations

⁵⁷ Ibid., 47.

⁵⁸ An alternative could be a centrally controlled cyber defense capability for all systems in the U.S.

and non-military events are linked more closely than before. Civilians will find they need greater understanding and detail of how the military plans to achieve its assigned objectives and what tools are to be used. This greater understanding will form the basis for a new whole-of-government approach.

Cyber will also alter the timing of the civilian-military integration, as this relationship shift is not just applicable in wartime. The civilian-military interaction must be present in peacetime as well; cyber operations require preparation. Unlike what is often seen in the media, new cyber operations are generally time intensive. It can take a considerable amount of time to determine what the system architecture of the adversary is and how to gain entry. A human element might be required to gain access to a system. Once entry is gained, an attacker must often study the system to determine how to achieve the desired effect. Finally, the attacker must build the offensive element or code and insert it. While at times this can be done quickly—generally on unsophisticated systems—this process will not normally be rapid. It is quite the opposite. Experts indicate that planning for a cyber-attack may require longer and have more intelligence requirements than a kinetic attack.⁵⁹ Consequently, operations must be planned, surveyed, and initiated in advance. This may require planning before hostilities are apparent, often in peacetime or while political decision-makers have not decided to commence hostilities or are not yet willing to admit to a possible future conflict. The types of activities required, if discovered, can have political consequences and will drive greater civilian involvement in military affairs during peacetime as policy-makers strive to control American policy. This will shift the American way of war to one in which civilians have greater control over the military—much to the angst of military desires.

⁵⁹ Lin, 44.

Use of Force Concepts

Cyber warfare will also continue to move the American way of war away from a distinct separation between the states of war and peace. Peacetime and wartime will no longer be exclusive states of existence in the American way of war. Activities normally associated with war will exist in peacetime. All of this is brought about by the addition of cyber and cyber warfare.

State-sponsored cyber activities are already emerging today during a state of peace: Stuxnet, Estonia, and Sony Pictures are just a few examples. The unresolved question is whether these actions are war or peacetime operations. A common answer is that maybe they are somewhere in the middle. A 2010 Chatham House report succinctly states the issue: “Cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict.”⁶⁰ In the American way of war, the state of war is characterized by armed conflict. But if cyber actions are a means to achieve goal without the use of force, then there may be a need to redefine “war” and “peace” that includes a shared space.

Cyber blurs the border between the conditions of war and peace by creating some of the same effects seen in wartime without the use of force. The anonymity, potential covertness, remoteness, and the aesthetic nature of operations are characteristics of cyber. Furthermore, proxies, such as cyber militias that may or may not be under government control, can take actions that could be considered acts of war. David Fidler refers to this blurry area where much of cyber warfare currently appears to reside as the ‘zone of ambiguity’. This zone “provides states and non-state actors with incentives to engage in

⁶⁰ Paul Cornish, David Livingston, Dave Clemente and Claire York. *On Cyber Warfare*. (London: Chatham House, 2010), vii.

or tolerate a range of activities in cyberspace...these activities face a lack of rules, controversies about what rules apply, or difficulties in making harmonized rules function.”⁶¹ Together these characteristics and ambiguous existence combine to make cyber operations easier for political decision-makers to undertake in peacetime.

America already embraces pre-emptive military actions. The characteristics of cyber warfare will continue to favor pre-emptive actions without the use of force, similar to the unattributed employment of Stuxnet. Combine America’s pre-emptive tendency with the relative ease of use, and cyber warfare activities are more likely in the future. This places America squarely in the zone of ambiguity and further pressures the American way of war to eliminate its black-and-white differentiation between peace and war.

This debate over cyber actions and their relationship to war will continue for the immediate future as individual nations develop their responses based on the context of each cyber action. Regardless of perspective on where cyber actions fall in the spectrum of war and peace, this blending of the two has implications for the evolution of American way of war. The ambiguity will end the apolitization of war common in the American way of war. If there is no distinction between war and peace, then activities in war, i.e. of the military, can no longer be shielded from politics. Instead, each action and its context will have political consequences. Therefore, civilian decision-makers cannot cede freedom of action to the military and must be more involved with military activities to establish and maintain the desired state of affairs. Actions, especially those taken in the zone of ambiguity, clearly affect the nature of the peace. Consequently, there is very

⁶¹ David P. Fidler. “*Inter arma silent leges* Redux? The Law of Armed Conflict and Cyber Conflict.” In *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 75.

little space in which the military can be ceded freedom of action when cyber warfare is involved.⁶² Cyber will alter the American way of war to not just view its actions as a political instrument, but to conduct them as such—with increased civilian involvement in military affairs to control the political linkage.

Military Forces, Civilians, and Collateral Damage

The American way of war includes going to extreme lengths to ensure that the effects of war are limited to the opposing military forces and government. Not only is this a desire of America, but the idea is also codified into international law. Activities in cyber, however, challenge America's ability to exclude civilians or civilian infrastructures from any effects of conflict because, again, there is no clear distinction between military and civilian in cyber.⁶³ Matt Crosston elaborates: "International laws on conventional warfare are effective because of the ability to differentiate between civilian and military sectors. There is a civilian/military ambiguity in the cyber domain that makes such differentiation unlikely if not impossible well into the future."⁶⁴ For example, if an adversary desired to disrupt America's military communications, it would find that much of the military's communications relies on commercial infrastructure—therefore, eliminating America's ability to communicate via cyber warfare would involve targeting civilian systems.⁶⁵ This is the dilemma with cyber: "previous assumptions about the nature of the international system—among them rationality, proportionality,

⁶² Point worthy of mention: in total war, it is possible that this space exists. Or, possibly in a clear state of war, at the tactical level, there are areas in which freedom of action in cyber would be available to the military to affect military systems.

⁶³ Cornish, et al. vii.

⁶⁴ Matthew Crosston. "Duqu's Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyber War" *Proceedings of the International Conference of Information Warfare & Security*. (International Security & Counter Terrorism Reference Center), 43.

⁶⁵ John Arquilla. "Twenty Years of Cyberwar." *Journal of Military Ethics* 12, no 1 (2013). 84.

predictability, and knowability—may no longer be operative.”⁶⁶ The trend in America’s way of war where collateral damage is continually minimized and civilians are insulated from the effects of war may be reversed with the addition of cyber.

In cyber warfare, when a state or military plans an attack, some form of the attack’s execution will travel through and involve commercial assets and networks.⁶⁷ Again, Crosston takes this one step further in stating that to “go after the ‘military’ targets, and you will also *de facto* be going after ‘civilian’ targets.”⁶⁸ This concept of interconnectedness and the indistinguishable nature of military and civilian systems are common throughout the cyber debate. Regardless, the dual-use of these systems, as David Fidler illustrates in his essay “*Inter arma silent leges Redux?*”, allows that attacking them “might be permissible if enemy forces utilize those systems for military purposes.”⁶⁹ This is similar to the current concepts of proportionality and necessity embedded in existing international law—even if the authors of the law did not envision such a lack of distinction between military and civilian.

This lack of distinction has the effect of making the attack’s design and the decision to execute more complicated. Nonetheless, the American way of war will still endeavor to limit collateral damage. Cyber actions will complicate this ability by introducing multiple forms of uncertainty. As mentioned earlier, significant intelligence on the targeted system will be required. Any errors or unknowns in that knowledge create “large uncertainties about direct and indirect effects of a cyber attack and will

⁶⁶ Jeffery R. Cooper, “A New Framework for Cyber Deterrence.” In *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 108.

⁶⁷ Crosston, 45.

⁶⁸ Ibid.

⁶⁹ Fidler, 80.

make it difficult for commanders to make good estimates of likely collateral damage.”⁷⁰

As Lin states: “the smallest change in configuration or interconnection of a computer system or network can result in a completely different system behavior.”⁷¹ In other words, what is not known about the system architecture or errors in understanding can create unanticipated collateral damage, limiting any ability to control such damage.

Additionally, human reactions to an attack can alter the way a cyber attack unfolds.⁷²

The system operators may or may not notice an attack. Different protocols executed by the targeted systems operators could have the effect of compounding, halting or spreading the attack. Even if the response protocol is known as part of the gathered intelligence, there is no way for the attack to be certain that the system operator will follow it.

Furthermore, despite precautions, collateral damage can come in the effects of blowback or spillover into American systems, both military and civilian, or neutral parties. These effects are not limited to the original attack vector either. For example, Stuxnet managed to infect systems around the globe despite the exceptionally narrow parameters built into the original code; and, once identified, the Stuxnet code was open to study and modification by third parties. Therefore “when considering the use of cyber force, policy-makers should emphasize the possibility of collateral damage from unforeseen spillover due to network connectivity.”⁷³ The internet is ubiquitous and ever changing. Unforeseen collateral damage can appear from unanticipated connections.

⁷⁰ Lin, 44.

⁷¹ Ibid., 46.

⁷² Ibid.

⁷³ Robert Belk & Matthew Noyes. “On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy.” Masters Thesis (2012), 114.

This can also “impose uncertainty onto other agencies, markets, and the public.”⁷⁴ Risk of unforeseen consequences also factors into the argument for an increased whole-of-government approach. The uncertainty creates a need to ensure other agencies are prepared for any possible disruptions—and their ability to deal with any spillover may affect policy-makers decisions to use cyber attacks. Finally, this spread of collateral damage is not just limited to inside America and neutral parties. Within the enemy state, knowledge of the interconnectedness of systems may be even lower, creating greater potential for spillover. While America will still attempt to limit collateral damage, with cyber, America will lose some of its ability to completely control the effects of a cyber attack.

There is another side to the collateral damage argument. Some experts view cyber as presenting opportunities for greater precision and less collateral damage than seen with kinetic weapons. Stuxnet, for example was a very precise weapon that had very little, if any, indirect collateral damage.⁷⁵ Ryan Jenkins argues that Stuxnet shows that “the most optimistic appraisal of cyber warfare is that it promises a way to vastly improve our abilities to satisfy the requirements of proportionality and discrimination.”⁷⁶ This potential future, if correct, would mesh perfectly with the American way of war and its increasing precision and continual reduction in collateral damage.

⁷⁴ Ibid., 121.

⁷⁵ The reader may note a contradiction with an earlier statement regarding Stuxnet. Stuxnet, in its original form was very limited in when it would become active. Even if Stuxnet spread from the original target, it would be dormant on non-targeted systems. Therefore Stuxnet itself is often considered a very precise “weapon”. However, as noted earlier, once Stuxnet was identified in the wild, it was eligible for modification. Stuxnet could then form the basis of new variants capable of infecting different types of systems and causing direct and indirect effects. This complexity in the context of cyber actions between precision and lack of control is a key factor in the uncertainty in the future environment.

⁷⁶ Ryan Jenkins. “Is Stuxnet Physical? Does it Matter?” *Journal of Military Ethics* 12, no 1 (2013), 75.

However, that path of extreme precision is only part of the future of cyber warfare. For as Herbert Lin demonstrated, the more precise the cyber weapon, the greater the intelligence requirements needed to create it.⁷⁷ Furthermore, the amount of time needed to gain intelligence and develop precise code is great. These types of situations are not easily created during war—they are more akin to peacetime, pre-emptive attacks or attacks early in a conflict that were prepared prior to hostilities. During war, users will likely increase protection on their systems; they may also make changes to architecture, isolating portions, or imposing strict controls in response to a perceived threat. Attacks requiring lengthy preparation are not likely to be common but rather to be rare, as time may not be available to the attacker. This increases the uncertainty in the effects of an attack.

The same theme of a lack of a demarcation between military and civilian cyber infrastructure also extends to civilian personnel. Crosston illustrates this point: “many of the actors that are part of planning, initiation, and deployment of cyber attacks are not necessarily formal military but civilian employees of government agencies.”⁷⁸ This is not just in America, but common in many nations. While this poses a dilemma within international law, these civilians can be legitimate targets if indeed they are filling a military combat function.⁷⁹ Maj Gen Charles Dunlap (Ret), former Deputy Judge Advocate General of the U.S. Air Force, argued that if a civilian was “sufficiently critical to military cyber operations” they could be attacked wherever they could be found, and collateral deaths in doing so would be allowed as long as they were not “excessive in

⁷⁷ Lin, 47.

⁷⁸ Crosston, 44.

⁷⁹ Charles J. Dunlap Jr. “Some Reflections on the Intersection of Law and Ethics in Cyber War.” *Air & Space Power Journal*, (January-February 2013), 29.

relation to the concrete and direct military advantage anticipated.”⁸⁰ In other words, the integration of cyber into warfare increases the involvement of civilians in warfare and also makes them legal targets. Traditionally targeted civilians were primarily the adversary’s leaders or were filling roles supporting the war effort and considered collateral damage during infrastructure attacks. With cyber, civilians fill the ranks of the ‘warfighters’ and can be legal targets. This may be especially true as states migrate to the use of cyber militias to undertake cyber attacks rather than place that capability into their respective militaries.⁸¹ This alters the perspective of the American way of war by broadening the concept of what “opposing military forces” are. The American way of war will need to evolve to a broader definition.

The American way of war will still attempt to insulate civilians from the effects of war and minimize collateral damage. While cyber may allow further gains in precision to do just that, the uncertainty of effects along with cyber’s blending of military and civilian infrastructure makes isolating effects to military targets a questionable assumption. For peacetime operations, sophisticated attacks such as Stuxnet have potentially demonstrated increased precision in operations. However, Stuxnet was an attack that evolved in stages over years.⁸² During war, the luxury of time is doubtful except for at the onset. Combatants will alter their systems, attacks will be constantly created, and the uncertainties of the effects will grow. For the American way of war, this means accepting this greater uncertainty to be inherent within cyber warfare. The American

⁸⁰ Ibid.

⁸¹ Richard B. Andres. “The Emerging Structure of Strategic Cyber Offense, Cyber Defense and Cyber Deterrence.” In *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 101.

⁸² Kimberly Zetter. *Stuxnet Missing Link Found, Resolves some Mysteries around the Cyberweapon*. February 26, 2013. <http://www.wired.com/2013/02/new-stuxnet-variant-found/all/> (accessed January 3, 2014).

way of war will also need to rectify its image of avoiding civilian casualties with one where civilians are increasingly legitimate targets. While this is not necessarily against the American way of war, it is contrary to the image America presents to the world and will need to be carefully managed.

Conclusion

There is no question that the use of cyber in warfare will become an integral part of the American way of war. The American way of war has a history of adopting new technology to solve its dilemmas at all levels of war. Cyber will provide another technological means for America to do just that. Cyber actions in warfare will also yield another path for America to achieve its goal of overwhelming the enemy, enroute to a decisive victory. Cyber actions will further enable the American way of war's desire to achieve capitulation via systemic paralysis.

Appearances can be deceiving however. While the addition cyber actions to warfare may appear to be a perfect fit in the American way of war, cyber's uniqueness will challenge the current American way of war. To operate effectively in war that includes cyber actions, the American way of war must move toward an integrated government approach to war—beyond the level of coordination seen in the whole-of-government approach today. Cyber's level of integration into society will further eliminate the distinction between the military and civilian spheres. This will drive continued or even further civilian control over military actions in both peacetime and war. The American-perceived binary distinction between the states of war and peace will also be altered by cyber actions in warfare. As cyber actions become a replacement for

the use of force or used in lieu of resorting to force, the line between war and peace is blurred. Not only will this change how the American way of war looks at conflict, but will also reinforce the requirement for an integrated governmental approach as well as increased civilian control over military actions. Finally, cyber actions in warfare will affect the American way of war's perceived control over casualties and collateral damage as uncertainty is increased with the addition of cyber actions. Over time, the integration of cyber and the combination of these effects will change the American way of war.

Despite these effects, the American way of war follows its own path and will integrate cyber activities as it prefers, likely in the same manner as it integrated previous technologies. Thomas Mahnken's conclusion on how the military integrates technology may turn out to be insightful: "although the culture of the U.S. armed services both shaped and was shaped by technology, the services molded technology to suit their purposes more often than technology shaped them."⁸³ This leads this author to believe that any changes to the American way of war caused by cyber will be gradual. Some may already be underway. Regardless, historically, a significant event or outside forcing function is required for radical changes to the American way of war to permanently take hold, if it changes at all.⁸⁴ The integration of cyber warfare alone will not likely be enough of a forcing function to create the outlined changes and make a shift in the near future. Therefore, these ideas are presented as a starting point for discussion. Only time will tell what changes occur to the American way of war as a result of cyber warfare—this is just one envisioned future.

⁸³ Mahnken, 219.

⁸⁴ Examples are: losing a war (Vietnam, Iraq—although one could argue the changes did not last much past the end of each war), Congressional action (e.g. Goldwater Nichols), etc.

Bibliography

- Andres, Richard B. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, by Derek S. Reveron. Washington D.C.: Georgetown University Press, 2012.
- Arquilla, John. "Twenty Years of Cyberwar." *Journal of Military Ethics* 12, no. 1 (2013): 80-87.
- Belk, Robert, and Matthew Noyes. "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy." Masters Thesis, 2012, 151.
- Bendrath, Ralf. "The American Cyber-Angst and the Real World--Any Link?" In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham, 49-73. New York, New York: The New Press, 2003.
- Boot, Max. "The New American Way of War." *Foreign Affairs* 82, no. 4 (July - August 2003): 41-58.
- Brigety, Reuben E. *Ethics, Technology and the American Way of War: Cruise Missiles and US Security Policy*. New York, New York: Routledge, 2007.
- Buley, Benjamin. *The New American Way of War: Military Culture and the Political Utility of Force*. New York, New York: Routledge, 2008.
- Canjar, R. E. "The Modern Way of War, Society, and Peace." *American Quarterly* (The Johns Hopkins Press) 36, no. 3 (1984): 433-439.
- Caplan, Nathalie. "Cyber War: the Challenge to National Security." *Global Security Studies* 4, no. 1 (Winter 2013): 93-115.
- Clarke, Richard A., and Robert K. Knake. *Cyber War*. New York: HarperCollins, 2010.
- Cohen, Eliot. "Kosovo and the New American Way of War." In *War over Kosovo: Politics & Strategy in a Global Age*, edited by Andrew J. Bacevich and Eliot Cohen, 38-62. New York: Columbia University Press, 2001.
- Cornish, Paul, David Livingston, Dave Clemente, and Claire Yorke. *On Cyber Warfare*. Chatham House, London: Chatham House, 2010, 38.
- Crosston, Matthew. "Duqu's Dilemma: The Ambiguity Assertion and the Futility of Santized Cyber War." *Proceedings of the International Conference on Information Warfare & Security*. International Security & Counter Terrorism Reference Center.

- Danzig, Richard J. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington D.C.: Center for a New American Security, 2014, 57.
- Davis, Paul K. *Deterrence, Influence, Cyber Attack, and Cyberwar*. Working Paper, National Security Research Division, RAND, 2014.
- Demchak, Chris. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, by Derek S. Reveron, 121-137. Washington D.C.: Georgetown University Press, 2012.
- Denning, Dorothy E. "Cyber-security as an Emerging Infrastructure." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Latham Robert, 25-48. New York, New York: The New Press, 2003.
- Department of Defense. "Department of Defense Strategy for Operating in Cyberspace." 2011.
- Dipert, Randall R. "Other-than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy." *Journal of Military Ethics* 12, no. 1 (2013): 34-53.
- Downes, Alexander B. "Desperate Times, Desperate Measures: The Causes of Civilian Victimization in War." *International Security* 30, no. 4 (Spring 2006): 152-195.
- Dunlap, Charles J. Jr. "Some Reflections on the Intersection of Law and Ethics in Cyber War." *Air & Space Power Journal*, January-February 2013: 22-43.
- Echevarria, Antulio J., II. *Reconsidering the American Way of War: U.S. Military Practice from the Revolution to Afghanistan*. Washington, D.C.: Georgetown University Press, 2014.
- *Toward an American Way of War*. Carlisle: Strategic Studies Institute, 2004.
- Entous, Adam, Jullian E. Barnes, and Carol E. Lee. "Resignation Capped Tense Year for Hagel." *Wall Street Journal*, November 26, 2014: A1.
- Fidler, David P. "Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, by Derek S. Reveron, 71-88. Washington D.C.: Georgetown University Press, 2012.
- Gray, Chris Hables. "Perpetual Revolution in Military Affairs, International Security, and Information." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham, 199-214. New York, New York: The New Press, 2003.

- Gray, Colin S. *Another Bloody Century*. Phoenix Paperback Edition, 2006. London: Orion Publishing Group, 2004.
- "Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?" In *Irregular Warfare: Strategy and Considerations*, edited by Arnold Milton and Walt Berkovski, 79-135. New York, New York: Nova Science Publishers, 2012.
- *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Strategic Study, Carlisle: Strategic Studies Institute, 2013.
- Hoffman, Frank. "Politics and the American Way of War (and Strategy)." *War on the Rocks*. November 2013. <http://warontherocks.com/2013/10/politics-and-the-american-way-of-war-and-strategy/> (accessed September 3, 2014).
- Ignatieff, Michael. "The New American Way of War." *The New York Review of Books*. July 20, 2000. <http://www.nybooks.com/articles/archives/2000/jul/20/the-new-american-way-of-war/?insrc=toc> (accessed October 23, 2014).
- Jenkins, Ryan. "Is Stuxnet Physical? Does it Matter?" *Journal of Military Ethics* 12, no. 1 (2013): 68-79.
- Latham, Robert, ed. *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York, New York: The New Press, 2003.
- "Introduction." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham, 1-21. New York, New York: The New Press, 2003.
- Lee, Wayne E. *Barbarians & Brothers: Anglo-American Warfare, 1500-1865*. New York, New York: Oxford University Press, 2011.
- Libicki, Martin C. "Cyberspace is not a Warfighting Domain." *I/S: U.S. Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 321-336.
- Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploration." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, by Derek S. Reveron, 37-56. Washington D.C.: Georgetown University Press, 2012.
- Linn, Brian McAllister. *The Echo of Battle: The Army's Way of War*. Cambridge, Massachusetts: Harvard University Press, 2007.
- "The American Way of War Revisited." *The Journal of Military History* 66, no. 2 (April 2002): 501-530.

- Mahnken, Thomas G. *Technology and the American Way of War*. New York, New York: Columbia University Press, 2008.
- Milton, Arnold, and Walt Berkovski. *Irregular Warfare: Strategy and Considerations*. Edited by Arnold Milton and Walt Berkovski. New York, New York: Nova Science Publishers, 2012.
- Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunitites and Power in a Virtual World*. Washington, D.C.: Georgetown University Press, 2012.
- Sondhaus, Lawrence. *Strategic Culture and Ways of War*. New York, New York: Routledge, 2006.
- Weigley, Russell F. *The American Way of War: A History of United States Military Strategy and Policy*. Indiana University Paperback Edition, 1977. New York: Macmillan Publishing, 1973.
- Yould, Rachel E. D. . "Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham, 74-100. New York, New York: The New Press, 2003.
- Zetter, Kimberly. *Stuxnet Missing Link Found, Resolves some Mysteries around the Cyberweapon*. February 26, 2013. <http://www.wired.com/2013/02/new-stuxnet-variant-found/all/> (accessed January 3, 2014).

Vita

Lt Col Lisa Nemeth is an officer in the United States Air Force. Lt Col Nemeth is a graduate of Army Command and General Staff College and the Army School of Advanced Military Studies where she was awarded a Master's Degree in Military Arts and Science. She also holds a Masters in Business Administration from Colorado State University. Lt Col Nemeth currently is a student at the Joint Advanced Warfighting School.